UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/872,797	06/01/2001	Stephen Paul Morgan	ARC920000133US1	4139

7590 04/14/2005

John L. Rogitz
Rogitz & Associates
Suite 3120
750 B Street
San Diego, CA 92101

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/872,797	**Applicant(s)** MORGAN ET AL.	
	Examiner Minh Dinh	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _12 January 2005_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-18_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-18_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _6/1/2001_ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 01/12/2005. Claim 1 has been amended.

Response to Arguments

2. Applicant's arguments filed 01/12/2005 have been fully considered but they are not persuasive. Regarding the rejection of claim 1, applicant argues that Asay does not disclose two certificates generated by respective CAs that are independent of each other (p. 6, 2nd par). Asay shows that a message comprises a device certificate and a subscriber's certificate (fig. 8). Asay further discloses that the device certificate is issued by the manufacture which is in a certification authority hierarchy (fig. 6, element 206; col. 37, lines 55-60) and that the subscriber's certificate can be issued by one of the sponsors (fig. 6, element 208; col. 32, lines 9-14). The sponsors, in addition to issuing certificates, also maintain and verify issued certificates; therefore, each sponsor is functionally equivalent to a CA (col. 32, lines 16-19; col. 33, lines 14-19). Figure 6 and lines 9-19 of column 32 shows that the certification authority hierarchy and the sponsors are two separate systems and independent of each other such that no trust relationship exists between them. Regarding applicant's argument with respect to the rejection of claim 7, Asay shows that a message comprises a device certificate and a subscriber's certificate (fig. 8). Accordingly, two IDs corresponding to the two certificates are needed for the ID payload.

Claim Objections

3. Claim 6 is objected to because of the following informalities: claim 6 has been amended to be dependent upon claim 5 instead of claim 4; however '4' has not been deleted. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harkins et al, "RFC 2409 – The Internet Key Exchange (IKE)", in view of Asay et al (5903,882).

Regarding claims 1-3 and 13-15, Harkins discloses a computer authentication protocol comprising sending a certificate payload from a sending computer to a receiving computer, the certificate payload including the sender's certificate (Section 3.2, Notation; Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose sending two certificates each being generated by a respective certificate authority (CA), the certificate authorities being independent of each other such that no trust relationship exists between the CAs. Asay discloses sending two certificates, the certificate of the subscriber together with the certificate of the host device (fig. 8). Asay further discloses that the device certificate is issued by the manufacture that is certified in a certification authority hierarchy (fig. 6, element 206; col. 37, lines 55-60) and that the subscriber's certificate can be issued by one of the sponsors (fig. 6, element 208; col. 32, lines 9-14). The sponsors, in addition to issuing certificates, also maintain and verify issued certificates; therefore, each sponsor is functionally equivalent to a CA (col. 32, lines 16-19; col. 33, lines 14-19). Figure 6 and lines 9-19 of column 32 shows that the certification authority hierarchy and the sponsors are two separate systems and independent of each other such that no trust relationship exists between them. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins protocol to send two certificates, the certificate of the sender together with the certificate of the host device, each certificate being generated by a respective certificate authority (CA), the certificate authorities being independent of each other such that no trust relationship exists between the CAs, as taught by Asay. The host device could be authenticated using the device's certificate (col. 36, line 64 – col. 37, line 11).

Regarding claims 4 and 16, Harkins discloses sending at least one identification (ID) payload between the computers, the ID payload including the sender's ID (Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose the ID payload being generated by combining the IDs of at least two entities; however, this feature is obvious by the combination of Harkins and Asay discussed above. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins protocol such that the ID payload is generated by combining the

IDs of two entities. Please refer to motivation recited for using two certificates for authentication as taught by Asay in claim 1.

Regarding claims 5 and 17, Harkins discloses sending at least one signature payload between the computers, the signature payload including the sender's signature (Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose the signature payload being generated by concatenating the signatures of at least two entities; however, this feature is obvious by the combination of Harkins and Asay discussed above. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins protocol such that the signature payload is generated by concatenating the signatures of two entities. Please refer to motivation recited for using two certificates for authentication as taught by Asay in claim 1.

Regarding claim 7, Harkins discloses a device comprising means for generating and sending an ID payload and a certificate payload from a sending computer to a receiving computer, the ID payload including the sender's ID, the certificate payload including the sender's certificate (Section 3.2, Notation; Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose sending a second ID and a second certificate associated with an entity different than the sender. Asay discloses sending the IDs and certificates associated with two entities, a sender and the host device (col. 32, lines 9-17; figure 6, elements 206, 208; and figure 8). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins device to send the IDs and certificates associated with both the sender and the host device, as taught by Asay. The host device could be authenticated using the device's certificate (col. 36, line 64 – col. 37, line 11). Accordingly, the ID payload includes the two IDs corresponding to the two certificates.

Regarding claim 8, Harkins discloses means for generating one signature payload including the sender's signature (Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose the signature payload being generated by concatenating the signatures of at least two entities; however, this feature is obvious by the combination of Harkins and Asay discussed above. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins device such that the signature payload is generated by concatenating the signatures of two entities. Please refer to motivation recited for using two certificates for authentication as taught by Asay in claim 7.

Regarding claim 10, Harkins discloses a device comprising means for generating and sending a signature payload and a certificate payload from a sending computer to a receiving computer, the signature payload including the sender's signature, the certificate payload including the sender's certificate (Section 3.2, Notation; Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose sending a second signature and a second certificate associated with an entity different than the sender. Asay discloses sending the signatures and certificates associated with two entities, a sender and the host device (col. 32, lines 9-17; figure 6, elements 206, 208; and figure 8). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins device to send the signatures and certificates associated with both the sender and the host device, as taught by Asay. The host device could be authenticated using the device's certificate (col. 36, line 64 – col. 37, line 11). Accordingly, the signature payload is generated by concatenating the two signatures.

Regarding claims 6, 9, 11 and 18, Harkins further discloses that a signature is formed by applying a pseudorandom function to at least the associated ID to render a result, and then encrypting the result with a private key associated with the entity represented by the ID (Section 5, Exchange, "To authenticate either ... HASH_R directly").

Regarding claim 12, Harkins discloses means for generating and sending an ID payload including the sender's ID (Section 5.1, IKE Phase 1 Authentication With Signature). Harkins does not disclose the ID payload being generated by combining the IDs of two entities; however, this feature is obvious by the combination of Harkins and Asay discussed in claim 10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Harkins device such that the ID payload is generated by combining the IDs of two entities. Please refer to motivation recited for using two certificates for authentication as taught by Asay in claim 10.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Project P710 - Security for the TMN X-Interface, EURESCOM

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
4/11/05

Gilberto Barron
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100